

Critical Incident Management (CIM)

12 June 2024

Key points

- Sound critical incident management depends on good preparation and planning. The preparedness steps you take before an incident happens will play a decisive role in the success of the management of the response
- Prepare and disseminate contingency plans and SOPs, conduct rehearsals and training for staff for likely CIM scenarios
- To improve coordination, in all aspects of planning and rehearsals include others who are likely to be involved depending on the likely scenarios – i.e. other Agencies, Partners, host government actors etc.
- Once an incident occurs, take immediate measures to protect yourself and others, alert first responders and others (in accordance with SOPs), alert others who could be endangered and then account for staff and report the incident as soon as you are able
- Post incidents consider after-incident care to address possible long-term negative effects related to the incident and conduct a review or lessons learned activity which prevent future occurrence or mitigate the impact of similar incidents

1. Overview

This entry outlines critical incident management and advises on good practices for managers. It focuses on the order of events, key actions, and the support systems and tools required to respond successfully.

A critical incident is an incident (or incidents) that seriously, and negatively, affects the safety of UNHCR staff, beneficiaries or assets. Critical incidents are often unforeseen, urgent and immediate and usually can cause serious harm to UNHCR staff, Partners, beneficiaries or assets. Critical incidents can take many forms, and can affect staff, forcibly displaced persons or others.

Effective Critical Incident Management builds organizational resilience and minimizes disruption of Operational activity. Conversely poorly managed or ineffective Critical incident Management is likely to create a negative impact on the operation and on staff. These impacts may be wide ranging and long term and impact negatively on the organization affecting reputational risk and ability to deliver.

Whilst critical incident management usually commences when the event occurs, many steps required to effectively manage the event must be taken or planned in advance. Therefore, contingency plans and standard operating procedures (SOPs) must be in place before a critical incident occurs. Plans should also consider procedures for supporting personnel after such incidents, as the long-term effect on the well-being of individuals can be significant without appropriate care.

Even the most thorough planning cannot altogether eliminate the risk of a critical security incident. When one occurs, lives may depend on taking prompt and appropriate action. Such action is possible only if preparations are made beforehand.

2. Relevance for emergency operations

The likelihood of critical incident occurrence is often higher for emergency operations due to the context and environment. However, the workload and demands on managers' time in emergencies carries the risk of neglecting preparation and planning for such incidents. Managers need to be aware of this and therefore actively conduct CIM planning activities and establish structures and procedures to manage incidents so that operations and protection of displaced and stateless people are not adversely affected.

Establishment of a Critical Incident Management Team (CIMT), with assigned roles and responsibilities, update of Contingency planning and SOPs and rehearsal for likely scenarios is key to effective management of significant critical incidents. Managers must allocate time to disseminate, explain and practice the agreed procedures with staff. Alternate members must also be considered in the absence of key incident managers.

3. Main guidance

Critical incident management (CIM) is the process whereby UNHCR offices manage an extraordinary event to ensure the least amount of damage to the organization and its staff while continuing operations.

The priority aims of the CIM process are:

- Save lives and protect wellbeing of personnel;
- Protect premises and assets;
- Minimize impact of safety and security crisis on programs and activities;
- Ensure preparedness and recovery from the impact of the critical incident.

CIM is a continuum and includes four sequential steps:

- Planning and Preparedness
- Initial Response
- Continuation (protracted situations)
- Recovery

Planning and Preparedness

In situations when a critical security incident has occurred, UNHCR's approach to security management emphasizes proactive planning, and some of the most important actions must be undertaken, or planned for, before the event occurs.

Important actions during the Preparedness and Planning Stage include:

- Regularly assessing risk and validating criticality of programs in high-risk areas, and ensuring operational posture is appropriate;
- Ensuring compliance with Security Risk Management (SRM) and Security Risk Management Measures (SRMM) and allocating resources for needed security improvements;
- Conducting preparedness, contingency and business continuity planning; -
- Ensuring managers in the field understand notification and reporting requirements, including the requirement to report critical security incidents immediately and maintain up to date personnel lists and other emergency information.

Initial Response

The initial response to Managing critical incidents involves convening the CIM structure to manage the information flow and make decisions on necessary actions. Recommended strategies include the use of the 'four boards concept' in which the management team charts four areas necessary for Critical Incident Management – What do we know? What do we need to know? What have we done? and What do we need to do?

Initial response includes the following immediate actions;

- Notify relevant Regional and HQ actors;
- Convene Critical Incident Management Team;
- Consolidate information available and Identify information gaps necessary for decision making;
- Take decisions based on facts or delay decisions if further reflection is necessary;

Continuation

Critical Incidents affecting UNHCR have often been protracted and in situations such as kidnapping could last up to six months or longer. In these situations, managers will need to establish an incident management routine to not adversely affect normal operations and to share workloads to avoid burnout and fatigue.

- Establish Critical Incident Management routine
- Maintain open Communication
- Report through regular updates

Recovery

Critical incident management for a particular incident will eventually end. It is important during recovery to reflect on what has happened and to document procedures that worked well and those areas where further improvement is necessary. Following a critical incident, threat and vulnerability analyses may change, necessitating a revised SRM and added Security Risk Management Measures (SRMM) and mitigation measures.

- Ensure a review of the Operational Posture;
- Review/Validate programme criticality and acceptable risk level;
- If necessary, conduct a lessons learned exercise;
- Conduct/participate in investigations and inquiries if appropriate;
- Take remedial Actions and follow up with affected staff members

CIMT Roles and Responsibilities

Critical Incident Manager

The CIMT manager ensures that CIM plans and structures are always in place and assumes overall management responsibility and decision-making. Depending on the incident's severity, the Bureau Director, the Representative or Head of Office may lead the CIMT as the Critical Incident Manager. In protracted incidents, or incident prone environments, this may not be possible, and a dedicated critical incident manager could be appointed.

Communications Officer - Reporting and Information

Messaging, reporting, information management, and liaison must be part of each CIM process and considered in plans and SOPs. Within the CIMT, the staff assigned the functional role of reporting and information must effectively communicate key messages to personnel. The focal point may also cover public information/external relations.

Security focal Point

The security focal point should be the most senior security officer of the operation to provide security related advice to the Critical Incident manager on security policies and procedures relevant to the incident, and coordinate and liaise with UNDSS and host government security entities. In significant incidents where the Regional Bureau Director is the Critical Incident Manager, usually the Security Focal Point will be the regional Senior Field security Coordinator (SFSC). The Security focal point will liaise with Field Security Service.

Operations and Programme

Experienced operations and programme staff serve as CIMT focal points to advise on re-directing activities, partners and resources to continue essential activities through business continuity planning.

Administration/Finance/HR

The focal point advises on administrative procedures relevant to the incident, contractual

options, and ensures that personnel lists and related information are always current. If the topics medical and staff welfare cannot be covered by the Admin/HR focal point, a dedicated focal point should be added to the CIMT.

Supply and Logistics

The focal point advises on available frame agreements or other contractual options regarding goods and services needed to respond to the incident and for operational continuity.

Critical Incident Management checklist

- Develop contingency plans and Standard Operating Procedures (SOPs) with input from stakeholders (multi-functional team approach) and partners to ensure compliance and effectiveness. Review and update your contingency plans regularly; modify them when necessary.
- The CIMT should practice critical incident management. One way is to conduct a table-top exercise, in which team members work their way through a fictional incident. Consider potential incidents based on the threats identified in the SRM process.
- Share, explain and practice contingency plans and SOPs with concerned staff to confirm their feasibility, or how to improve them, and to achieve familiarity.
- During a critical incident, take decisions as necessary, seek advice from subject matter experts or entities that can provide additional support i.e. Medical Services, FSS, Legal Affairs Section (LAS), Inspector General's Office (IGO). Engage with specialists employed to support the Critical Incident e.g. Hostage Incident Management (HIM) team.
- Ensure timely flow of accurate information to all members of the crisis management team and to entities that play any role in supporting management of the incident.
- Post Incident ensure return to normal operational delivery as soon as possible. Ensure follow-up with staff members affected - be aware some may be affected after the incident's conclusion.

- When necessary, conduct after action review and lessons learned exercise. Ensure gaps identified are incorporated into revision of existing plans.

4. Policies, Guidelines and Useful Links

5. Links

[Security Management Operations Manual \(UN Security Management System\)](#)
[UNHCR/AI/2017/04/Rev.1 Administrative Instruction on Medical Evacuation and Oth...](#)

6. Main contacts

UNHCR Field Safety Section (FSS), Division of Emergency, Security and Supply (DESS). At:
HQFS00@unhcr.org